**INFORMATION SYSTEM SECURTIY**

**ASSIGNMENT 1**

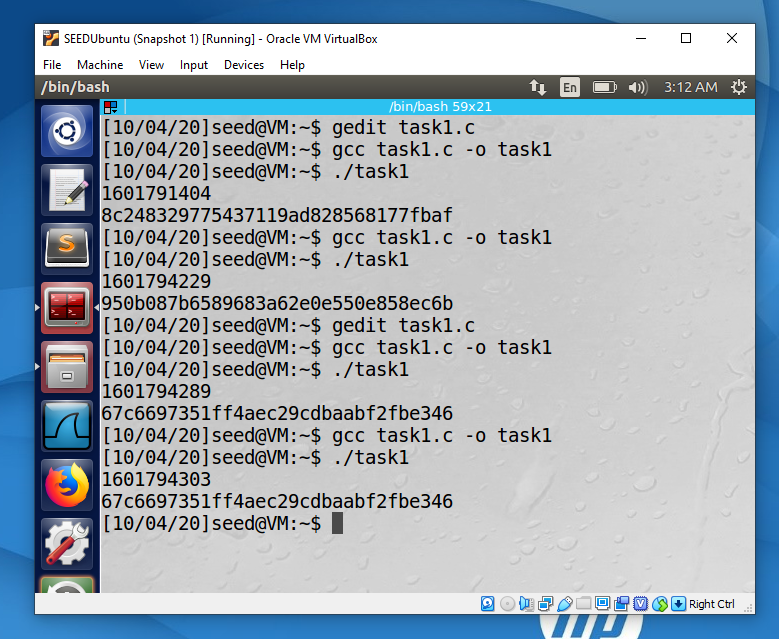
PSEUDO RANDOM NUMBER GENERATION LAB

**Name:** Ayesha Ausaf

**Roll No:** 17k-3867

**Section:** F

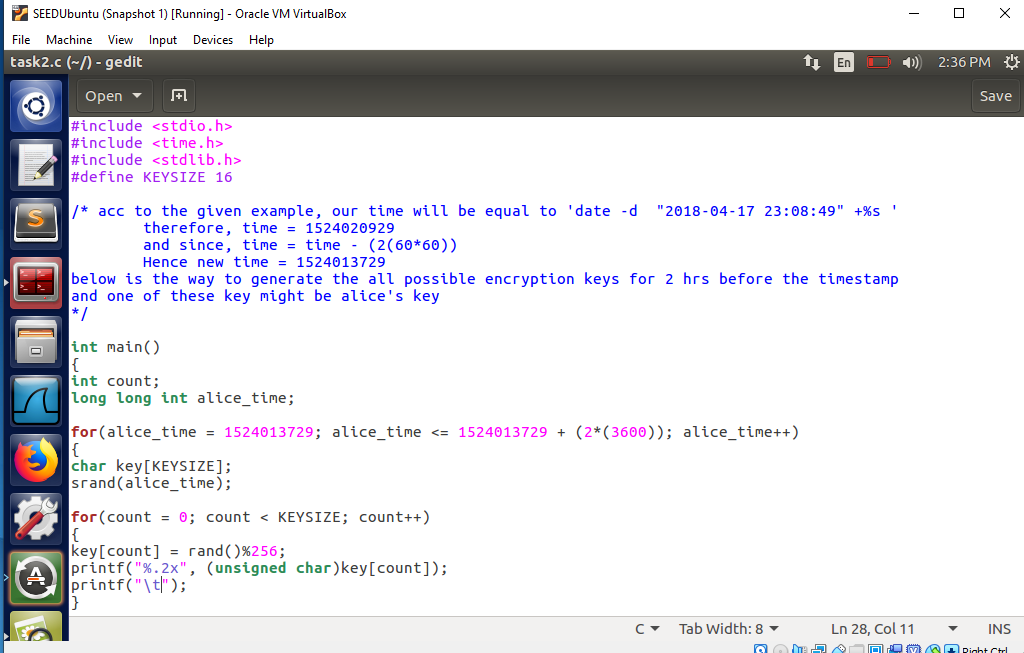
**Task 1**



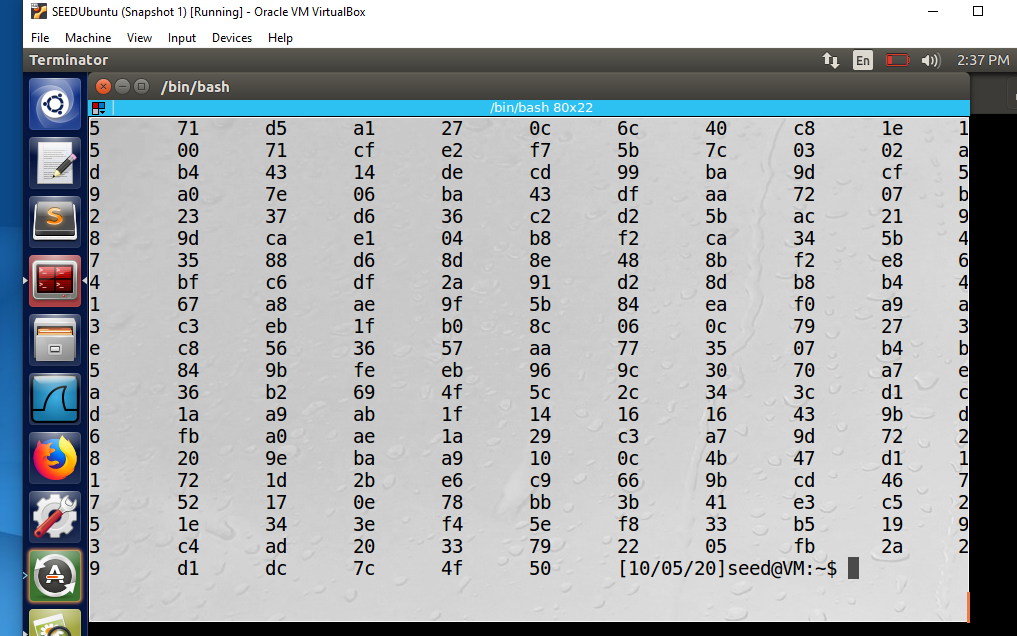
When we run the program using the whole given code for first time, it takes the current time from pc and using the srand() function on time, it picks a random seed from the time as a starting point and then generate a series of random numbers. So every time we run the program, a unique key is generated as the time changes (as shown in the first 2 outputs on terminal). Whereas, when we run the program after commenting out line 1, same key is generated every time as we run the program (as shown in the last 2 outputs on terminal).

**Task 2**

Code for finding possible keys:

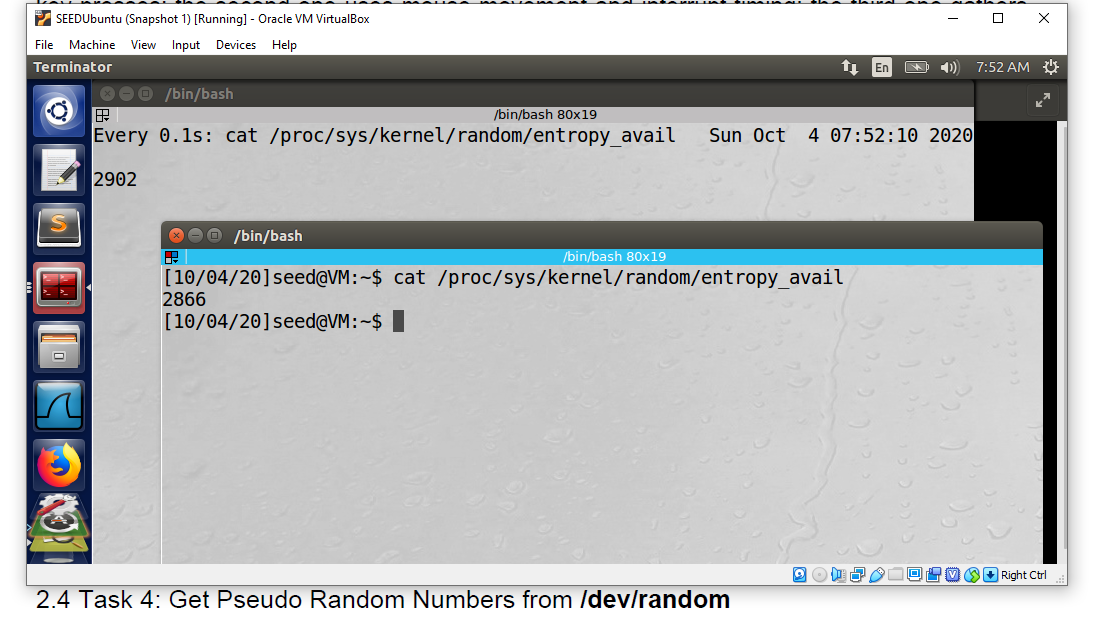


Desired output:



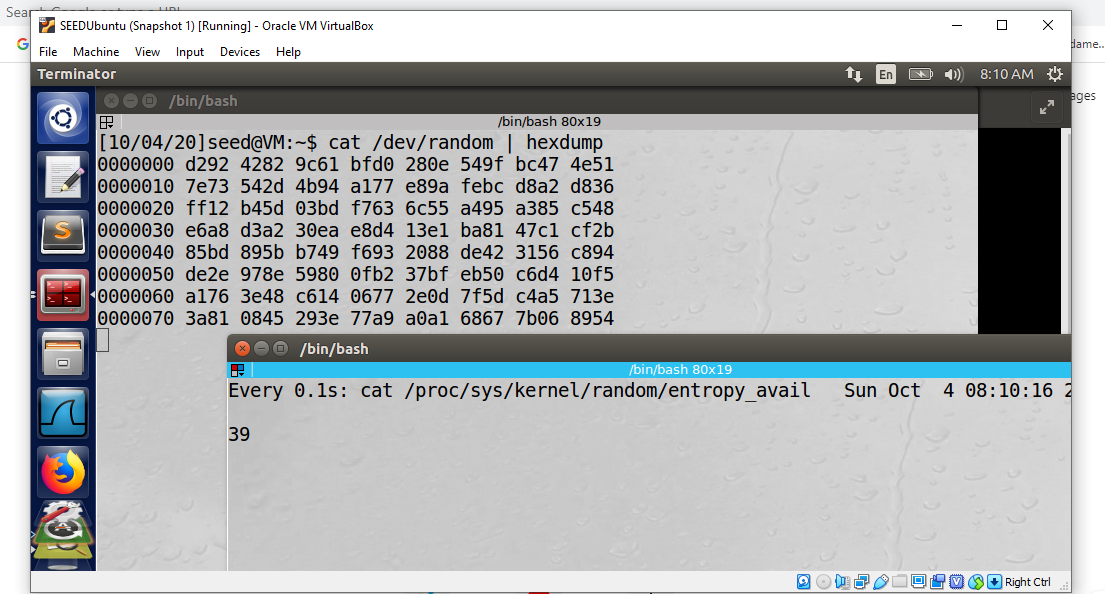
**Task 3**

From what I observed, moving the mouse and typing something increases the entropy slowly (2 units or 3 units). Whereas, clicking somewhere using the mouse increases entropy by 4 units (a bit faster than moving the mouse), and reading a large file or visiting a website increases the entropy significantly.



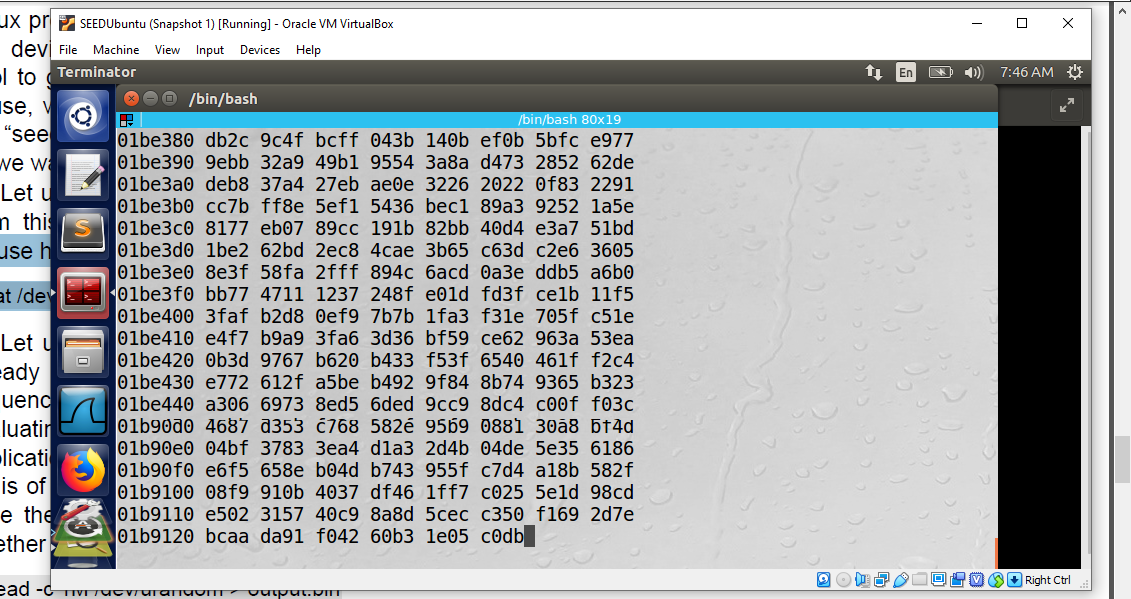
**Task 4**

If I am not moving the mouse, the entropy will increase by 1 unit after every 0.1 s, but when I move the mouse, entropy is increasing rapidly i.e. (1 unit increase by a single move), but the entropy resets itself after reaching between 50 to 60 and also resets itself after every output of the hexdump.



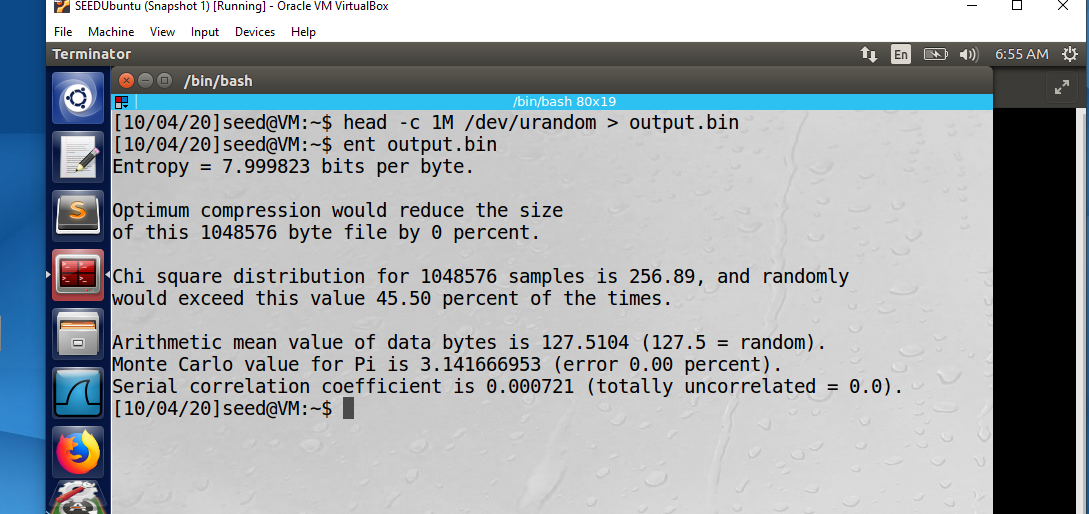
**Task 5**

Part 1:



There is no change in the output when the mouse is moved.

Part 2:



Entropy – optimum compression: The file is dense in information i.e. random.

Chi-Square – This a good quality of random number because the percent value is lesser than 90%.

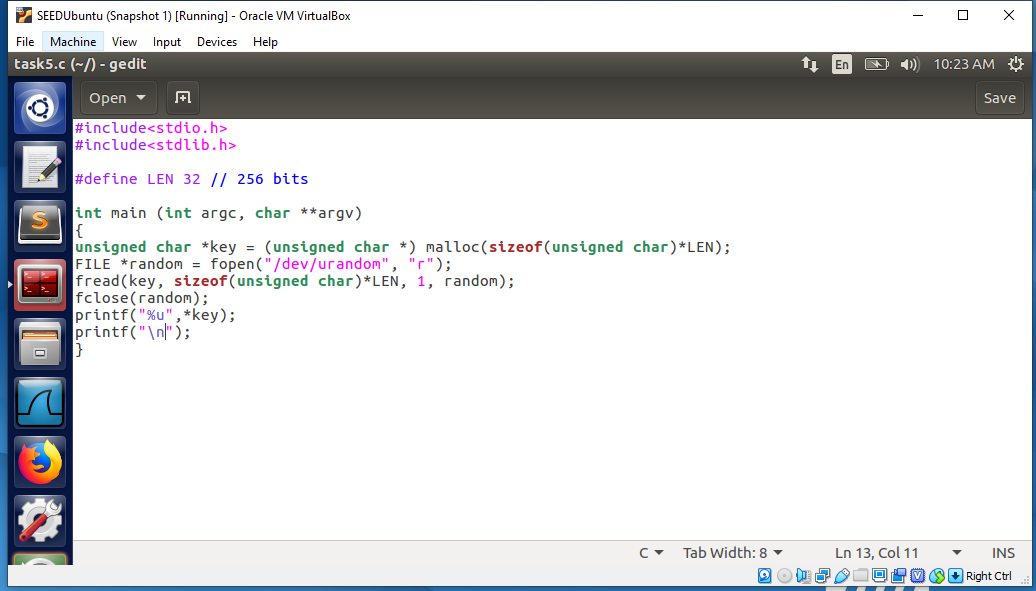
Arithmetic mean - The value suggests that the data is close to random.

Monte Carlo - Data is closest to random as there is 0 error and pi value is exact.

Serial correlation coefficient - It is a random sequence as the value is near to 0.

Part 3:

Modified code:



Desired output:

